Aktenzeichen XY gelöst – Forensische Analyse realer Cyberangriffe deckt Taktiken der Angreifer auf

Sophos Active Adversary Report for Tech Leaders 2023: Detaillierte Untersuchung der vom Sophos Incident Response Team übernommen Fälle macht deutlich, dass Angreifer immer kürzer im infiltrierten Netzwerk verweilen, bevor sie ihre Attacke starten, sie zudem weniger als einen Tag benötigen, um auf das Active Directory zuzugreifen und die Mehrheit der Ransomware-Attacken außerhalb der Geschäftszeiten stattfinden.

Wiesbaden, 23. August 2023 –Sophos veröffentlicht heute seinen Active Adversary Report for Tech Leaders 2023. Der Bericht gibt einen detaillierten Einblick in das Verhalten und die Tools von Angreifern im ersten Halbjahr 2023. Auf Basis der Analyse der von Sophos bearbeiteten Incident Response (IR)-Fälle von Januar bis Juli 2023 hat Sophos X-Ops herausgefunden, dass die durchschnittliche Verweildauer von Angreifern (Zeit vom Beginn eines Angriffs bis zu seiner Entdeckung) bei allen Angriffen von zehn auf acht Tage und bei Ransomware-Attacken auf fünf Tage gesunken ist. Im Vergleichszeitraum im Jahr 2022 sank die Verweildauer von 15 auf 10 Tage.

Hohe Gefahr für die Kronjuwelen eines Netzwerks
Sophos X-Ops fand außerdem heraus, dass Angreifer im Durchschnitt weniger als einen Tag – etwa 16 Stunden – benötigten, um das Active Directory (AD) zu erreichen. Das AD verwaltet in der Regel die Identitäten und den Zugriff auf Ressourcen in einem Unternehmen. Der Zugriff der Angreifer auf das AD bedeutet, dass sie die Privilegien in einem System erweitern und eine Vielzahl von schädlichen Aktivitäten durchführen können.

„Ein Angriff auf das Active Directory eines Unternehmens ist aus cyberkrimineller Sicht sinnvoll. Das AD ist in der Regel das leistungsstärkste und privilegierteste System im Netzwerk und bietet einen umfassenden Zugang zu weiteren Systemen, Anwendungen, Ressourcen und Daten, die Angreifer für ihre Angriffe ausnutzen können. Wenn ein Angreifer das Active Directory kontrolliert, kann er das gesamte Unternehmen kontrollieren. Dieses Eskalationspotential und der hohe Wiederherstellungsaufwand eines Active Directory sind die Gründe, warum es so gezielt angegriffen wird", sagt John Shier, Field CTO bei Sophos.

Den Active-Directory-Server in der Angriffskette zu erreichen und die Kontrolle darüber zu erlangen, bietet Angreifern mehrere Vorteile. Sie können unbemerkt verweilen, um ihren nächsten Schritt zu planen. Sobald sie bereit sind, dringen sie ungehindert weiter in das Netzwerk des Opfers ein. Die vollständige Wiederherstellung einer kompromittierten Domäne kann ein langwieriger und mühsamer Prozess sein. Ein solcher Angriff beschädigt die Sicherheitsgrundlage, auf die sich die Infrastruktur eines Unternehmens stützt. Sehr oft bedeutet ein erfolgreicher AD-Angriff, dass ein Sicherheitsteam bei Null anfangen muss.

Ransomware: Kürzere Verweildauer und Angriffe außerhalb der Geschäftszeiten
Die Verweildauer bei Ransomware-Angriffen ist gesunken. In den analysierten IR-Fällen waren sie mit 69% die häufigste Angriffsart und die durchschnittliche Verweildauer betrug nur fünf Tage. Bei 81% der Ransomware-Angriffe wurde der endgültige Schadcode außerhalb der üblichen Arbeitszeiten gestartet. Von den Angriffen, die während der Geschäftszeiten ausgeführt wurden, fanden nur fünf an einem Wochentag statt.
Die Zahl der entdeckten Angriffe nahm im Verlauf einer Woche zu, vor allem bei der Untersuchung von Ransomware-Angriffen. Fast die Hälfte (43%) der Ransomware-Angriffe wurde entweder am Freitag oder am Samstag entdeckt.

„In gewisser Weise sind wir Opfer unseres eigenen Erfolgs. Mit der zunehmenden Verbreitung von Security-Technologien und -Diensten wie XDR und MDR lassen sich Angriffe früher erkennen. Eine kürzere Erkennungszeit führt zu einer schnelleren Reaktion, was wiederum zu einem kürzeren Zeitfenster für Angreifer führt. Gleichzeitig haben Kriminelle ihre Schachzüge optimiert, insbesondere die erfahrenen und gut ausgestatteten Ransomware-Ableger, die ihre Angriffe angesichts der verbesserten Verteidigungsmaßnahmen weiter beschleunigen. Das heißt aber nicht, dass wir insgesamt sicherer sind. Dies zeigt sich am Einpendeln der Verweildauer auf einem hohen Niveau bei Nicht-Ransomware. Angreifer dringen immer noch in Netzwerke ein, und wenn die Zeit nicht drängt, verweilen sie dort. Alle Security-Tools der Welt werden Unternehmen nicht retten, wenn sie nicht aufpassen und Systeminformationen nicht richtig interpretieren. Es braucht sowohl die richtigen Tools als auch eine kontinuierliche, proaktive Überwachung, um sicherzustellen, dass die Kriminellen am kürzeren Hebel sitzen. MDR kann die Lücke zwischen Angreifern und Verteidigern schließen, denn selbst wenn das Unternehmen einmal nicht aufpasst, passen wir auf", sagt Shier.

Über den Sophos Active Adversary Report for Tech Leaders
Der Sophos Active Adversary Report for Business Leaders baut auf weltweiten Sophos Incident Response (IR)-Daten aus 25 Branchen von Januar bis Juli 2023 auf. Die angegriffenen Unternehmen befanden sich in 33 verschiedenen Ländern auf sechs Kontinenten. Achtundachtzig Prozent der Fälle stammten von Unternehmen mit weniger als 1.000 Mitarbeitern.
Der Sophos Active Adversary Report for Tech Leaders bietet Sicherheitsexperten Daten über Bedrohungen sowie Erkenntnisse, um ihre Sicherheitsstrategie besser zu operationalisieren.

Um mehr über das Verhalten, die Tools und Techniken von Angreifern zu erfahren, lesen Sie "Time Keeps on Slippin' Slippin': The 2023 Active Adversary Report for Tech Leaders," von Sophos.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.
Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de